State of Illinois

Department of Central Management Services

SHARED SERVICES GLOSSARY

Standard

Effective January 30, 2007

Public Distribution
Version 1.0

Shared Services Glossary

Effective January 30, 2007

Version 1.0

APPROVAL SHEET

EXPEDITED APPROVAL

BCCS Deputy Director: ___________________________ Date: __________

If approved digitally (via email), attach copy & write subject line & date below.

Owner: ___________________________ Date: __________

If approved digitally (via email), attach copy & write subject line & date below.

Policy Review Board Chair: ___________________________ Date: __________

If approved digitally (via email), attach copy & write subject line & date below.

Return to Policy Review Board Chair

Expedited publications MUST be formally submitted to the Policy Review Board within 180 days from the BCCS Deputy Director approval date in order to undergo customary review and stakeholder comment or the publication will be withdrawn and retired.

CMS Shared Services
GLOSSARY

Activation

A CMS recovery term identifying the plan containing specific instructions to restore a resource. A sample template can be found at the Recovery Services SharePoint site http://cmsteam.illinois.gov/sites/bccs/rm/dr/public/default.aspx.

Agency

Used generically to represent any governmental entity. An entity's formal, full name may contain the words agency, board, commission, council, department, task force, or not (as in Illinois State Police). State agencies have taxing authority to collect revenue within the state of Illinois or they receive state appropriations from the Illinois Legislature. Per Illinois State statute 20 ILCS 405, state agency means "all departments, boards, commissions, and agencies of the State of Illinois subject to the Governor." Agency may also refer to an organization within the federal government such as Homeland Security, the General Accounting Office, or the Federal Emergency Management Agency.

Agency Abbreviation

BCCS Business Services maintains an abbreviation for each agency, board, commission, and taxing authority in Illinois government. This list is used as the BCCS standard.

Appropriate Business Unit

An organizational group within or outside CMS that has authority, responsibility, or has been delegated the responsibility for a particular task or function.

Approved Use

Authorized access to a resource granted by the resource custodian or other authorized designee for an official business use. Any action that meets the definition of "inappropriate" is not an approved use action.

Authorized / Unauthorized

Authorized means approved by policy, published procedure, appropriate management-level person, or by the custodian or custodian designee. Authorization may be granted through written documentation or by default of official, written job duties or properly signed contractual agreement.

Unauthorized means not authorized. That is, unauthorized is any action or user that is not authorized to access, view, copy, intercept, use, or otherwise interact with a state resource.

Authorized User

Individuals or entities assigned resource privileges by the resource owner or custodian and accessing only those resources for which they have been granted access.

Availability	The assurance that a resource is accessible, usable, and functional when needed. The ability of an IT Service or configuration item to perform its agreed function when required. *(ITIL)*
BCM	Within ITIL, acronym has 2 different meanings: Business CAPACITY Management or Business CONTINUITY Management
BIA	see Business Impact Analysis
BRM	Business Reference Model. An internally developed BCCS database containing information on major state computer applications.
Business Continuity	Processes that identify potential impacts that threaten an organization and provides a framework for effective responses that safeguards the interests of the organization. Also, the management of recovery or continuity in the event of a disaster or the management of the overall program through training, rehearsals, and reviews, to ensure the plan stays current and up to date. *(DRII)* Manages risks to ensure that at all times an organization can continue operating to, at least, a predetermined minimum level. (*ITIL*)
Business Impact Analysis	BIA. Determines what impact levels to a system are tolerable. (*Sans Institute)*. A Service Continuity Management activity that defines recovery requirements for services & identifies vital business functions & dependencies. *(ITIL)*
Change	To become different, to pass/transform from one stage or state to another. Change as a process is managed by BCCS Change Management and formal procedures.
Classification	Classification refers to the hierarchical structure of organizing data and information for the purpose of applying controls (risk mitigation, access, and security). Data is classified into *confidential*, *sensitive*, and *public*.
CMS	Illinois Department of Central Management Services. CMS' mission is to free Illinois governmental entities to empower them to focus their resources on core missions. CMS provides a variety of commonly shared services such as procurement, personnel employment & benefits, facilities (property) management, fleet (vehicle) management, information technology, telecommunication, and videoconferencing.

CMS / BCCS	Bureau of Communications and Computer Services. BCCS provides data processing and telecommunications services to state agencies and operates the state's central computer facility. BCCS manages a secure, statewide telecommunications network, available 24x7 that serves more than 800 cities in all 102 Illinois counties. BCCS also serves as the state Internet service provider for all state agencies, boards, and commissions.
COBIT	Control OBjectives for Information and related Technology. A framework that is internationally accepted as best practices for control over information and IT related risks. It is 100% compliant with ISO17799, COSO, and maps to many other standards. It is also used as a tool to meet regulatory compliance including the Sarbanes-Oxley Act. COBIT bridges the communication gap between IT, business, and auditors by providing a common approach, understandable by all. The Illinois Office of the Auditor General applies COBIT criteria when conducting audits of CMS operations.
Confidential	Confidential information includes any knowledge that could place an individual or entity at risk of harm, damage, or financial loss. Within ITIL's Security Management area, the security principle that requires that data should only be accessed by authorized people. *(ITIL)* Confidential data includes but is not limited to HIPAA protected health information, Freedom of Information Act Exemptions, network specifications, or client/customer identifiable data.
Confidentiality	The protection of data and information that prevents its unauthorized access, disclosure, dissemination, or distribution.
Confidentiality Disclaimer	Placed on a fax or e-mail to protect the sender and the state from erroneous delivery. *This electronic transmission and any attached files contain information for the exclusive use of the individual or entity to whom it is intended and properly addressed and may contain information that is proprietary, privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any viewing, copying, disclosure, or distribution of this information is strictly prohibited and may be subject to legal restriction or sanction. If you have received this communication in error, please notify the sender, by electronic mail or telephone, and delete the original and all copies of the message.*

Contingency Plan

A plan to respond to a specific systems failure or disruption of operations. May use any number of resources including workaround procedures, alternate work area, a reciprocal agreement, or replacement resources. (*DRII*)

Continuity Management (IT Services)

A process that supports the overall business continuity process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support, and service desk) can be recovered within required timeframes. (*ITIL*)

Continuity Of Operation Plan

(COOP)

Provides guidance on system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. Term traditionally used by the Federal Government and its supporting agencies to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning. (*DRII*)

Crisis Management

The overall coordination of an organization's response to a crisis (critical event), which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate), in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's ability to operate. (*DRII*)

Critical

Use of the word “critical” is avoided when referencing recovery priorities. Recovery priorities are defined by the *stage* in which a business function is recovered. Stage is determined by the degree of impact and the business function’s recovery time objective (RTO).

Custodian

A person or entity that guards and protects or maintains. *(Merriam-Webster Online Dictionary)*

Data/ Information

For use in State of Illinois Central Management Services policies and procedures, data and information are used interchangeably. Both are considered resources and intangible assets.

When necessary to make a distinction,

DATA shall mean: meaningless characters (letters, numerals, special symbols,, etc) rendered in a form suitable for processing by an electronic device or in a format/structure where no association or interpretation can be made to derive a meaning or significance which could lead to information.

INFORMATION shall mean: any communication or representation of knowledge or meaningful facts, figures, statistics, opinions, etc. in any form including but not limited to verbal, audio, hand-written, mechanical, graphical, printed, or electronic and may be separate from the media on which it resides. Information is data that is assigned an association or interpretation that results in meaning or knowledge.

Defense-in-Depth

The practice of layering defenses to provide added protection by placing multiple barriers between an attacker and information resources. A defense-in-depth strategy achieves information assurance through a balanced focus on people, technology, and operations.

Disaster

Per the International Information Systems Security Certification Consortium (ISC2), disaster is any sudden, unplanned calamitous event that brings about great damage or loss.

In the context of business operations, a disaster is any event creating an inability to deliver critical business functions or that negatively impacts meeting the organizations' mission.

Disaster Recovery

DR. Used here to differentiate between business continuity (all encompassing recovery) and DR (recovery limited to IT related resources).

Activities and programs designed to return a business function to an acceptable condition. The ability to respond to an interruption and restore an organization's critical business functions. *(DRII)*

Disaster Recovery Plan

The management approved document that defines the resources, actions, tasks and data required to manage the recovery effort. Usually refers to the technology recovery effort and is a component of a business continuity management program. (*DRII*)

DR

see Disaster Recovery.

DRII	Disaster Recovery Institute International (DRII), formed in 1988, sets standards that provide the minimum acceptable level of measurable knowledge that provides a baseline for levels of knowledge and capabilities in areas of disaster recovery and business continuity. DRII is the industry’s certification authority promoting a base of common knowledge for the business continuity planning/disaster recovery industry through education, assistance, and publication of the industry's international standard “Professional Practices for Business Continuity Planners”.
DRJ	Disaster Recovery Journal. A publication dedicated to the continuity and recovery field with over 60,000 subscribers and sponsor of two annual conferences.
Due Diligence	Legal Definition: a measure of prudence, activity or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent person under the particular circumstances. Per Merriam-Webster Online Dictionary, “the care that a reasonable person exercises under the circumstances to avoid harm to other persons or their property.”
Electronic Vaulting	Electronically forwarding backup data to an offsite server or storage facility. Vaulting eliminates the need for shipment of physical storage media (tape, cartridges, CD, etc.) and therefore significantly shortens the time required to move data offsite
FISMA	The Federal Information Security Management Act of 2002 (FISMA), consists of Title III of the E-Government Act of 2002 (U.S. Public Law 104-347). FISMA outlines a mandate for improving the information security framework of federal agencies, contractors and other entities that handle federal data (i.e., state & local governments). FISMA consists of a set of directives governing what security responsibilities federal entities have, and it outlines oversight and management roles to the implementation of those directives
FOIA	Freedom of Information Act. Illinois state statute 5 ILCS 140, *Freedom of Information*, requires that all information generated and maintained by state entities - with explicit exceptions identified in Section 7 of the statute - must be openly available to the public upon written request. Refer to end of this glossary for the specific wording of Section 7 exemptions.
FY	Fiscal Year. For the State of Illinois, fiscal year is July 1 through June 30.

Governance

Within CMS, officially rolled-out on August 1, 2005, the IT/Telecom Governance Model is a set of political processes, driven by principles, and sponsored by Enterprise leaders to ensure that IT investments are optimized and meet the objectives of:

- Alignment of IT/Telecom with enterprise goals & realization of promised benefits
- Use of IT/Telecom to enable the enterprise to take advantage of opportunities
- Optimize use of IT/Telecom resources
- Management of IT/Telecom-related risks

Per COBIT, IT Governance is a "structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes."

Guideline

General statement covering discretionary recommendations designed to achieve a policy's objective by providing a framework within which to implement controls not covered by a procedure. (*ISC2)*

High Availability

A service or business function needed to be available 24x7. Results of a business impact analysis and risk assessment demonstrate that comprehensive damage and risk will result when a high availability service or application becomes unavailable for more than 2 hours. Sufficient redundant components are specifically designed, implemented, and deployed to maximize availability

Impact

The magnitude of harm caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential impact to the agency mission. (NIST 800-30)

Impact can be expressed in terms of loss of confidentiality, integrity, and/or availability, in specific dollar amounts (quantitative), or qualitative terms such as high, moderate, or low.

Note that the Institute of Risk Management uses the term 'consequences' whereas the State uses 'impact'. Refer to "Determining Impact Value" at the end of this document.

Inappropriate

Actions that violate and contradict state or federal law, state policy, or published procedural instruction.

Examples of inappropriate disclosure include but are not limited to the verbal or written communication of confidential data (as defined by the circumstance) to unauthorized individuals or entities, knowingly allowing unauthorized access to confidential information, or knowingly attempting access to an unauthorized resource for the purpose of gaining unauthorized information.

Examples of inappropriate use include but are not limited to knowingly accessing a resource for which there is no justified business need (user is not authorized) or the writing, display, or downloading of material considered by the state to be obscene, sexually explicit, offensive, political in nature, or otherwise derogatory to any race, sex, religion, or natural origin.

Incident

An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. *(NIMS)*

Incident Action Plan

An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods. (*NIMS)*

Information/ Data

For use in State of Illinois Central Management Services policies and procedures, data and information are used interchangeably. Both are considered resources and intangible assets.

When necessary to make a distinction,

DATA shall mean: meaningless characters (letters, numerals, special symbols,, etc) rendered in a form suitable for processing by an electronic device or in a format/structure where no association or interpretation can be made to derive a meaning or significance which could lead to information.

INFORMATION shall mean: any communication or representation of knowledge or meaningful facts, figures, statistics, opinions, etc. in any form including but not limited to verbal, audio, hand-written, mechanical, graphical, printed, or electronic and may be separate from the media on which it resides. Information is data that is assigned an association or interpretation that results in meaning or knowledge.

Integrity

The assurance that changes to data, information, applications, and processes are as intended and expected and that unauthorized or erroneous changes are prevented or at a minimum detected and corrected.

ISACA	Information Systems Audit and Control Association (ISACA), formerly the EDP Auditors Association, established in 1969, is the global organization for information governance, control, security and audit professionals. Its IS auditing and IS control standards are followed by practitioners worldwide. It is the certification body for more than 40,000 professionals holding the Certified Information Systems Auditor (CISA) designation. ISACA's membership numbers more than 47,000 worldwide, in more than 140 countries. ISACA publishes the Information Systems Control Journal and hosts a series of international conferences focusing on technical and managerial topics pertinent to the IS assurance, control, security and IT governance professions.
ISC^2	The International Information Systems Security Certification Consortium, Inc. (ISC)^2 is a non-profit organization that maintains the Common Body of Knowledge(CBK) for information security, and is the certification authority for the Certified Information Systems Security Professional (CISSP) professional designation with over 35,000 members in over 100 countries
ISO 17799	An internationally recognized standard comprised of a comprehensive set of controls embracing best practices in information security published and sponsored by the International Standards Organization.
IT	Information Technology.
IT Resource	Any logical or physical object used to create, store, manipulate, transfer, display, or delete data. Any methodology, technique, software, application, process, hardware, equipment, device, or combination that transforms data into information, transfers data from one location to another, displays data, or otherwise deals with, manipulates, or accesses data. Examples include but are not limited to computers, Blackberries, servers, mainframes, source code, databases, computer files, word documents, spreadsheets, Internet, e-mail, instant messaging, text messages, etc. as well as information itself.
ITIL	IT Infrastructure Library. A globally accepted approach to IT service management providing a cohesive set of best practices supported by the British Standards Institution's standard for IT service Management (BS15000). CMS is adopting ITIL as a governance model in the delivery of IT services to client agencies.
JCL	Job Control Language. Used in a mainframe environment to contain instructions executed by the operating system when running computer programs.

Knowledge	Application of information to solve a problem or improve a process. Also, experience and "know-how". Knowledge is considered a valuable asset and resource that must be managed. Knowledge can be tacit (undocumented) or explicit (documented, codified, written down).
Logical	Items that are intangible, dealing with reasoning, analysis, logic, knowledge, etc. A logical IT resource, for example, includes data, files, databases, records, computer programs, software, operating systems, applications, etc.
Mean Time Between Failures (MTBF)	A metric for measuring & reporting reliability defined as the average time that an IT Service can perform its agreed function without interruption measured from when the IT Service starts working until it next fails. *(ITIL)*
Mean Time Between Service Incidents (MTBSI)	A metric used for measuring & reporting reliability defined as the mean time from when a system or IT Service fails until it next fails. Calculated as equal to MTBF + MTTR. *(ITIL)*
Mean Time To Repair (MTTR)	A metric for measuring & reporting maintainability defined as the average time taken to restore an IT Service after a failure and measured from when the IT Service fails until it is fully restored & delivering normal functionality. *(ITIL)*
Methodology	A CMS recovery term identifying the plan containing strategic decisions necessary to restore shared service capabilities. One methodology may govern several activation plans. More information is available from the Recovery Services site http://cmsteam.illinois.gov/sites/bccs/rm/dr/public/default.aspx
Mitigation	Per the Disaster Recovery Institute, implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner. Per NIMS, activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident.
MTBF	see Mean Time Between Failures
MTBSI	see Mean Time Between Service Incidents

MTTR

see Mean Time To Repair

National Incident Management System

NIMS. A system mandated by Homeland Security Presidential Directive 5 providing a consistent nationwide approach to recover from incidents. *NIMS*

A comprehensive, national approach to incident management applicable at all jurisdictional levels and across functional disciplines. NIMS provides a consistent nationwide template to enable all government, private-sector, and non-governmental organizations to work together during domestic incidents.

NIMS

see National Incident Management System.

NIST

National Institute of Standards and Technology, founded in 1901, is a federal government agency within the U.S. Commerce Department's Technology Administration with a mission to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST programs include:

- NIST Laboratories which conducts research to advance the nation's technology infrastructure to continually improve products and services;
- Baldrige National Quality Program which promotes performance excellence among U.S. firms and recognizes quality achievement; and
- Advanced Technology Program which accelerates development of innovative technologies for broad national benefit by co-funding research and development partnerships with private sector organizations.

OA Coordinator

An Office Automation (OA) Coordinator is an individual identified by CMS/BCCS to be responsible for certain, specialized user-related IT functions. OA Coordinators assist end-users, in conjunction with the Customer Solutions Center personnel, in the resolution of computing and telecom problems.

OAG

Illinois Office of the Auditor General. Appointed by the Illinois Legislature, the Auditor General conducts an annual review of data processing controls at CMS on behalf of CMS client agencies.

Owner

To have power over a resource; to determine how a resource is to be used, allocated, protected, accessed, etc.

An owner is responsible for establishing rules of appropriate use and protection.

The state owns assets and resources purchased, acquired, and used to deliver state services.

Custodians are designated and assigned ownership duties such as access authorization, protection against unauthorized use, and integrity verification.

Physical

Anything that is tangible, touchable, has a material existence, and can be measured by weight, length, height, etc. A physical IT resource, for example, includes electrical, optical, or wireless equipment, hardware, or device such as a router, server, workstation, Blackberry device, printer, telecommunication cable, satellite, etc.

Plan

Documented steps, actions, processes, procedures, etc. that anticipate a particular event or consequence and attempts to reduce any negative impact.

For an explanation of the different types of plans, refer to the NIST Continuity Plan Relationships model at the end of this glossary.

Policy

DOCUMENT: High level statement of enterprise beliefs, goals, & objectives and the general means for their attainment. A policy is brief & set at a broad level. In conjunction with but separate from policy, an organization should publish procedures & standards that offer a consistent method of implementing policy. (*ISC2)*

OPERATIONS: A rule or set of guidelines applied to a device to ensure operation follows a predefined pattern.

Political

As used in policy and procedure guides, political relates to non-business subject areas including but not limited to specific party platforms, agendas, or activities; personal views or opinions on governmental issues, elected or appointed officials, or actions thereof; and any government related issue not directly impacting or related to your assigned job duties.

Political does not include state or federal legislation that has a direct impact on your assigned job duties.

Preparedness	The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Preparedness is a continuous process that identifies threats, determines vulnerabilities, and identifies required resources. Preparedness focuses on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification, and equipment certification. *NIMS*
Prevention	Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention applies intelligence to a range of countermeasures and deterrence operations such as heightened inspections, improved surveillance and security operations, investigations to determine the full nature and source of the threat, etc. *NIMS*
Probability of Occurrence	The possibility of a threat occurring; in a manual risk assessment, expressed as low, moderate, high. Refer to "Determining Probability Value" at the end of this document.
Procedure	Instructions that spell out step-by-step specifics of how a policy and supporting standards will actually be implemented. (*ISC2)*
Production	The state of an IT service or configuration item that directly or indirectly supports a BCCS business function that fulfills a need identified in a service level agreement or published mission statement.
Protected Health Information	Individually identifiable health information transmitted or maintained in any form or medium, which is held by a covered entity or its business associate. Identifies the individual or offers a reasonable basis for identification. Is created or received by a covered entity or an employer. Relates to a past, present, or future physical or mental condition, provision of health care or payment for health care. (HIPAA)
Public	A data classification category where information is accessible to or shared by all members of a community. Please note: "a community" when applied to the Internet, means world-wide, all people, foreign and domestic.
Public Information Officer	The only individual authorized and assigned the authority to coordinate the dissemination of information to news media and the public. Interacts with the public, news media, or with other agencies to deliver information for release to the public. (*NIMS, DRII, & FEMA)*

Reasonable Personal Use

Reasonable Personal Use are actions **limited** to those which:

- do not interfere or conflict with official state business, and
- do not adversely affect efficiency or effectiveness, and
- do not place unreasonable stress on any state resource, and
- results in negligible expense to the state, and
- are non-offensive to others, and
- are not for the purpose of commercial (personal profit making) gain, and
- is not otherwise prohibited, illegal, or unethical.

Recovery

The reconstitution of government operations and services. (*NIMS)*

The returning of an IT service to a working state. *(ITIL)*

Recovery Plan

A plan developed by a state, local, or tribal jurisdiction with assistance from responding Federal agencies to restore the affected area. (*NIMS)*

Recovery Point Objective

RPO. The point in time to which systems and data must be recovered after an outage. (e.g. end of previous day's processing). RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the systems or functions have been recovered. (*Disaster Recovery Institute*)

Recovery Time Objective

RTO. The period of time within which systems, applications, or functions must be recovered after an outage. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. Also known as maximum allowable downtime. *(DRII)*

Maximum time allowed for recovery following an interruption. *(ITIL)*

Release

Per ITIL, a collection of hardware, software, documentation, processes, etc. required to implement one or more approved changes to IT Services that are managed, tested, and deployed as a single entity.

Resource Type

For ease of classification, prioritization, relocation, and reference, agency resources will be identified as one of the following types:

- People (staff, technical experts, vendors, clients)
- Logical (Data, Source Code, Object/Load Libraries, Interfaces, etc.)
- Operational/Equipment/Mechanical
- Financial (Procurement)
- Power
- Communication (internal/external, voice, data, network)
- Transportation (air, rail, highway, road/street)
- Environmental System (heating, cooling, ventilation)
- Location (Building or Area Accessibility)

Resource Management

A system for identifying available resources to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Includes mutual-aid agreements and use of special teams. *NIMS*

Resource

Personnel, business partners, vendors, data/information/knowledge (stored in computer files, on paper, & in other storage media), financial appropriations, applications, software, equipment, supplies, and facilities available or potentially available for assignment and/or allocation to a state function or process during normal, day-to-day operation as well as to emergency/incident response.

Response

Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. *NIMS*

Revoke

Revoke means to disable, make non-useable. For a network or mainframe ID, the ID remains defined to the system but is not usable.

Risk

The combination of the probability of an event and its consequences (Institute of Risk Management)

The product of the level of threat with the level of vulnerability establishing the likelihood of a successful attack. (*Sans Institute)*

The negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk is a function of the likelihood of a threat exercising a vulnerability and the resulting impact of the adverse event on the organization. (NIST SP800-30).

The possibility of suffering harm or loss calculated as how likely it is that a specific threat will exploit a particular vulnerability. *(ITIL)*

The probability that a particular threat will exploit a particular vulnerability.

The potential for harm or loss expressed as answers to: (*ISC2*)

- what could happen? (what is the threat?)
- how bad can it be? (what is the impact/consequence?)
- how often might it happen? (what is the frequency?)
- how certain are the answers? (what is the degree of confidence?)

Risk Assessment

The overall process of risk analysis and risk evaluation. (*Institute of Risk Management*)

The process by which risks are identified and the impact of those risks determined. (*Sans Institute)*

The first process in a risk management methodology used to determine the extent of potential threats associated with an asset/resource (NIST SP800-30)

An examination of an organization's resources (assets), existing controls, and vulnerabilities combining the loss potential for each resource (or combination of resources) with an estimated rate of occurrence to establish a potential level of damage in dollars or other assets. (*ISC2*)

The initial step in risk management in which asset value is analyzed & threats identified & evaluated as to how vulnerable each asset is to those threats. *(ITIL*

Identification of threats and associated vulnerability and for each threat/vulnerability pair, determination of the impact upon confidentiality, integrity, and availability and the likelihood of the vulnerability exploit. (federal CMS Information Security Risk Assessment Methodology)

Risk Management

The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level (NIST SP800-30).

The continuous process of ever increasing complexity of the overall evaluation of the impact of exposures and the response to them. Includes phases of risk assessment and safeguard selection. (*ISC2*)

The process responsible for identifying, assessing, & managing risks. *(ITIL)*

A strategic, continuous management process where risks are methodically addressed with the objective of identification and treatment of risks to add maximum sustainable value to all activities within the organization. (Institute of Risk Management)
Includes prioritization of risks, categorization of recommended safeguards, implementation feasibility, and other risk mitigation solutions. (federal CMS Information Security Risk Assessment Methodology)

Risk Treatment

The process of selecting and implementing measures to modify the risk. Primary means by which risk is currently managed. Major elements are control/mitigation measures and treatment strategies. (Institute of Risk Management)

Best practice approaches include:
Accepting/Assuming, Sharing, Transferring, or Mitigating the risk.

For example, ITIL risk treatment options include:

- Applying cost effective controls to reduce the risk
- Deciding to accept the risk
- Avoiding the risk, by preventing the situation that could lead to it
- Transferring the risk to a third party, for example by taking out insurance.

Risk Level

A value subjectively entered or mathematically computed denoting the magnitude of a risk. For example, a value of low, moderate, or high may be assigned and/or numerical weights may be applied in a calculation based on a management-approved formula using probability of occurrence and impact.

The product of the likelihood of occurrence and the impact severity *(Centers for Medicare & Medicaid Services Security Risk Assessment Methodology)*

Refer to “Determining Risk Level Value” at the end of this document.

RPO

see Recovery Point Objective.

RTO

see Recovery Time Objective.

SANS

Established in 1989 as a cooperative research and education organization, the SANS (SysAdmin, Audit, Network, Security) Institute is a well respected and recognized source for information security training and certification. SANS maintains a large collection of research documents about various aspects of information security; operates the Internet's early warning system (the Internet Storm Center); and connects more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share lessons learned and solutions to the challenges they face. SANS resources include a weekly vulnerability digest (@RISK), weekly news digest (NewsBites), the Internet's early warning system (Internet Storm Center), flash security alerts and more than 1,200 award-winning, original research papers are free to all who ask.

Secured Resource

A resource that has some form of protection applied to it. Protection includes but is not limited to logical passwords, physical locks, and/or being located in a limited/controlled access facility (building). Most State Resources are secured. The major exception is public information, information displayed on public web sites, and information and documentation not exempt under the Freedom of Information Act.

Security Screening

Security screenings (background checks) are conducted in order to provide an initial risk assessment based on results from inquiries directed to the Illinois Secretary of State and a criminal history check through the Law Enforcement Agency Data System (LEADS).

LEADS provides Illinois and federal conviction information, Wants or Warrants, gang members affiliation and orders of protection.

Sensitive

Information that has the potential to cause embarrassment, humiliation, or dishonor to a person or entity.

An example of sensitive information is payroll information since this information may be obtained from the Comptroller's Office and is considered public information after proper Freedom of Information Act forms have been submitted.

SME

Subject Matter Expert. An individual with detail knowledge about a business function and/or its IT support. A SME may be a "power user", technician, or someone with a great deal of experience on a specific topic.

Social Engineering

An attack based on deception.
According to the International Information Systems Security Certification Consortium, the certification organization for IT security professionals, social engineering is defined as “attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network, or data”.

Stage

The order or phase in which a resource is recovered. Stage is a value ranging from 0 to 4 representing the sequence and time period in which a resource is restored at an alternate site. Stage is determined by the degree of impact and the business function’s recovery time objective (RTO). Refer to the Recovery Stage information below for more details.

Stakeholder

All people who have an interest in a project, activity, service, business function, etc. and may include customers, partners, employees, contractors, etc. *(ITIL)*

Standard

A specific product, mechanism, action, or rule applied universally throughout an organization in order to support and implement policy. (*ISC2*)

A mandatory requirement, code of practice, or specification published by a standards organization. *(ITIL)*

State Resource

A State of Illinois resource is any physical or logical item, tangible or intangible asset that is:

- purchased, leased, created, or maintained with State of Illinois funds;
- used in the delivery of state services regardless of funding source;
- used in meeting a state mission, initiative, goal, objective, or normal business operation.

Items may include but are not limited to any physical device, equipment, furniture, written documentation, etc. as well as any logical data, information, software, application, process, etc.

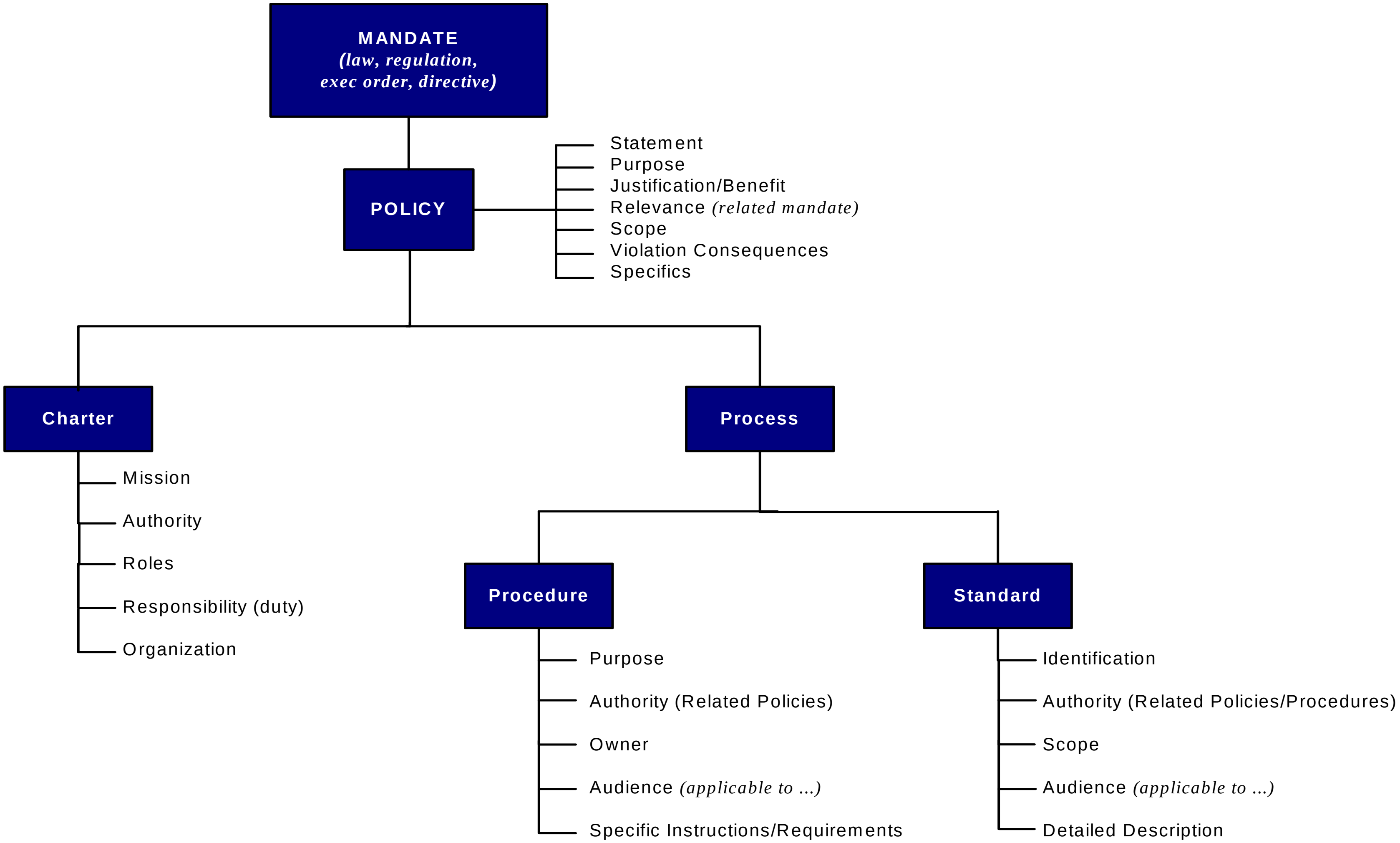
SWDC

StateWide Data Collection. The CMS business process that collects, manages, and disseminates IT recovery data at a statewide level.

Threat	An event, the occurrence of which could have an undesirable impact on the well-being of an asset (*ISC2*) The potential for a particular threat-source to successfully exercise a particular vulnerability. Threat-source is any circumstance or event with the potential to cause harm to an asset; includes natural threats (flood, earthquake, tornado, electrical storm, etc.), human threats (data entry errors, hacking, unauthorized access, etc.), and environmental threats (power failure, pollution, chemical spills, etc.) (NIST SP800-30)
Total Cost of Ownership (TCO)	A methodology used in investment decisions that incorporates entire lifecycle costs of a configuration item and not just the initial purchase price. *(ITIL)*
TVD	Technical Validation Database. A BCCS internal database that identifies all shared service hardware and relates it to software running on that hardware.
User	Any person or entity that uses a resource; any person or entity that receives a benefit from a resource.
Vulnerability	A weakness that can be exploited. *(NIST SP800-30 & ITIL)* The absence or weakness of a risk-reducing safeguard. A condition that has the potential to allow a threat to occur with greater frequency, greater impact, or both. (*ISC2*)
Whistleblower	Both the federal Whistleblower Protection Act and the Illinois Whistleblower Reward and Protection Act protect employees who alert law enforcement or other appropriate third parties to potentially illegal/unlawful actions. Under the Whistleblower Protection Act, whistle blowing is defined as disclosing information that an employee reasonably believes is evidence of illegality, gross waste or fraud, gross mismanagement, abuse of power, or a substantial and specific danger to public health and safety.

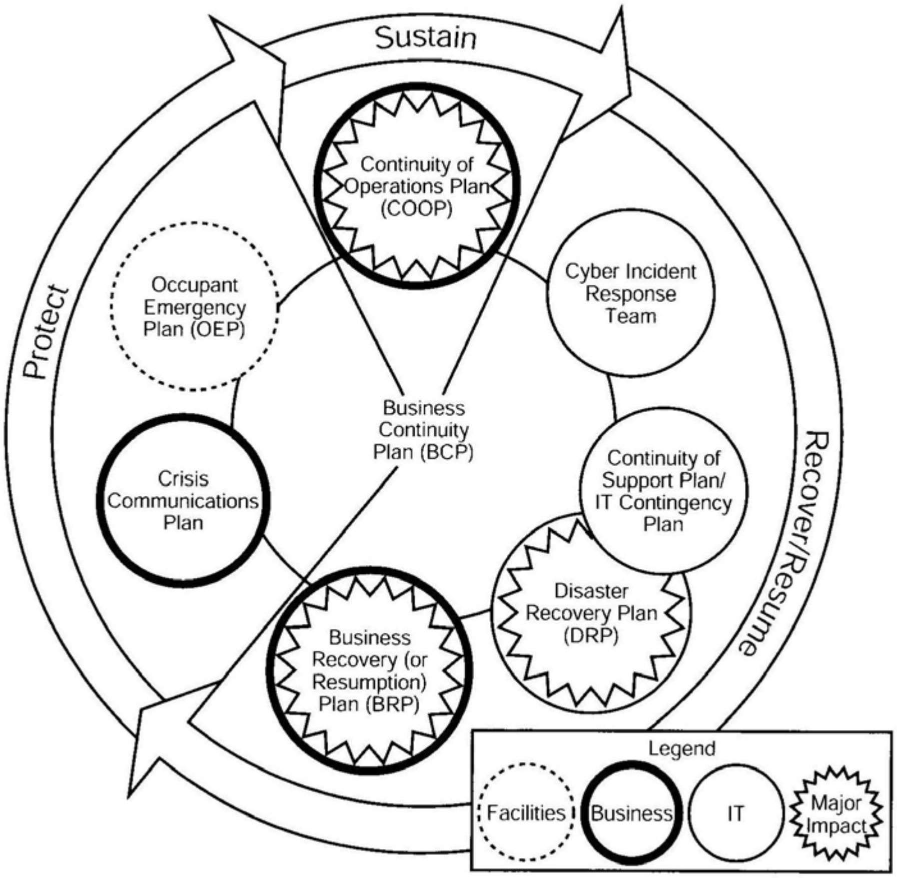
CMS/BCCS Shared Services
GLOSSARY

Policy, Process, Procedure, Standards Relationship


MANDATE
(law, regulation, exec order, directive)
POLICY
Statement
Purpose
Justification/Benefit
Relevance *(related mandate)*
Scope
Violation Consequences
Specifics
Charter
Mission
Authority
Roles
Responsibility (duty)
Organization
Process
Procedure
Purpose
Authority (Related Policies)
Owner
Audience *(applicable to ...)*
Specific Instructions/Requirements
Standard
Identification
Authority (Related Policies/Procedures)
Scope
Audience *(applicable to ...)*
Detailed Description

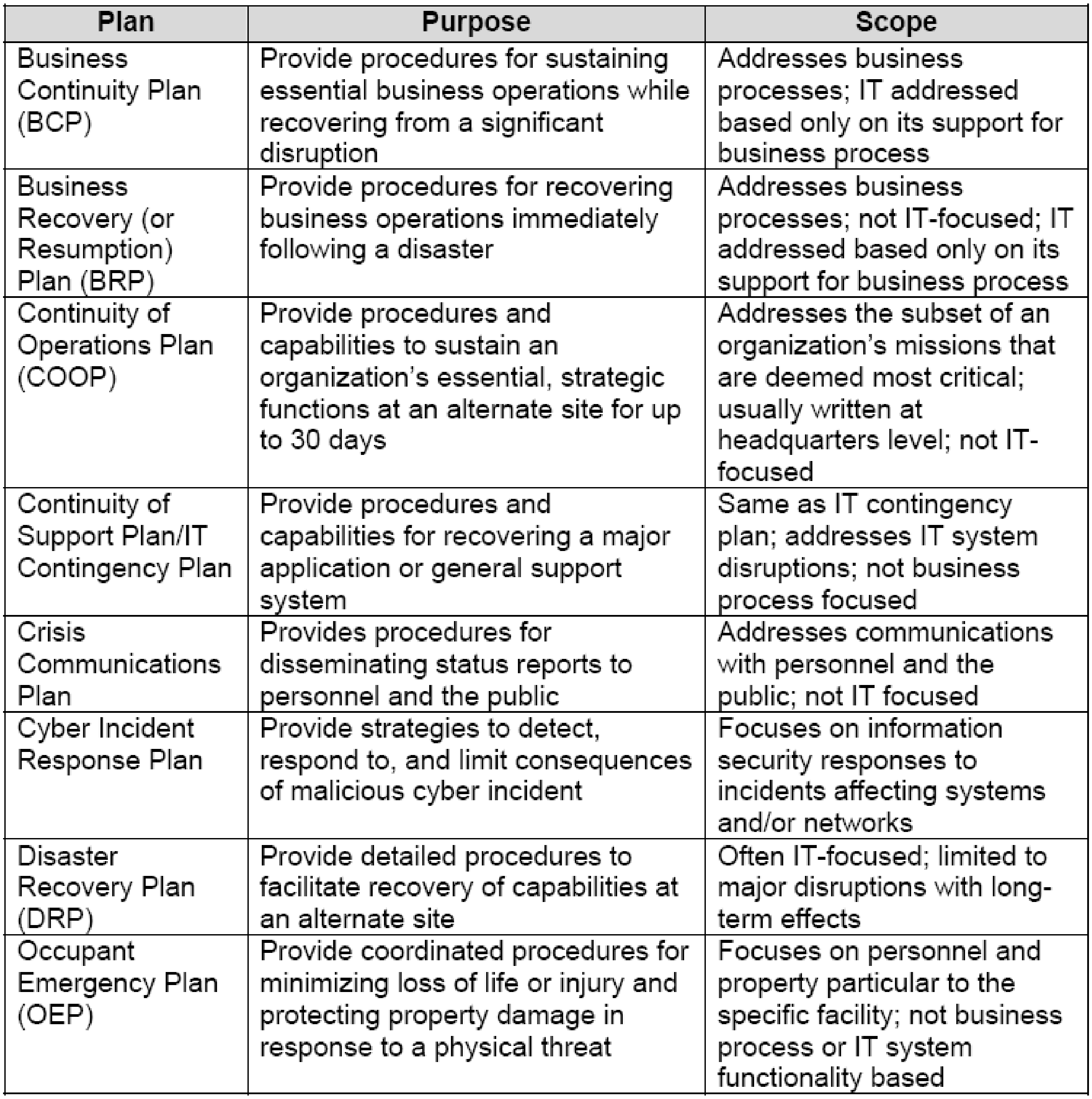
All documentation contains 1) Revision History and 2) instructions on who to contact to submit comments/suggestions/questions
No individual reference is made to a glossary/dictionary because there will be an enterprise glossary/dictionary containing all necessary abbreviations & terms
Audience is not limited to people. Audience may apply to hardware, software, or any other resource.

NIST Continuity Plan Relationships Graphic


Sustain
Protect
Recover/Resume
Continuity of Operations Plan (COOP)
Occupant Emergency Plan (OEP)
Cyber Incident Response Team
Business Continuity Plan (BCP)
Crisis Communications Plan
Continuity of Support Plan/ IT Contingency Plan
Disaster Recovery Plan (DRP)
Business Recovery (or Resumption) Plan (BRP)
Legend
Facilities
Business
IT
Major Impact

source: NIST Special Publication 800-34,
Contingency Planning Guide
for Information Technology Systems
pg 11

NIST Continuity Plan Relationships Matrix



Plan	Purpose	Scope
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption	Addresses business processes; IT addressed based only on its support for business process
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster	Addresses business processes; not IT-focused; IT addressed based only on its support for business process
Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days	Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system	Same as IT contingency plan; addresses IT system disruptions; not business process focused
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public	Addresses communications with personnel and the public; not IT focused
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident	Focuses on information security responses to incidents affecting systems and/or networks
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site	Often IT-focused; limited to major disruptions with long-term effects
Occupant Emergency Plan (OEP)	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat	Focuses on personnel and property particular to the specific facility; not business process or IT system functionality based

RECOVERY STAGES

CMS restores IT processing and communication capabilities in a phased, orderly approach referred to as *stages*. Stage is defined as a numerical value ranging from 0 to 4 representing the recovery phase (tier, order, priority) in which the business function will be restored. Because an IT capability is linked to a business function, the stage of the business function is the recovery priority of the IT capability.

A recovery time objective (RTO) must be assigned to each business function in order to assign a recovery stage to that business function. The RTO is assigned based on impact (as identified in a business impact analysis) and the risk level (as identified in a risk assessment).

Listed below is the recovery time objective (RTO) for each stage.

RECOVERY PRIORITY MATRIX

RECOVERY PRIORITY	**RTO (hours)**	
Stage 0	< 1	Rollover, Synchronous, Redundant
Stage 1	< 24	Requires recovery before mainframe SLA minimum
Stage 2	< 72	Can be recovered after mainframe restored
Stage 3	< 168	Must be restored within a week
Stage 4	> 168	Can forego IT services for 1 week or more
Periodic	Applied to resources that are sensitive to a specific business cycle or time period such as end of the month processing, end of fiscal or calendar year processing, or other times such as cutting client checks on the 10th of each month.	
Long Range	No need to recover until processing resumed at permanent site (*may have a sufficient manual/alternate process to accommodate business need until normal operation is resumed*)	

Agencies fill-in the Effect and Unavailability columns of the Impact Matrix.

This is a summary chart only and NOT a substitute for a detailed, comprehensive business impact analysis.

IMPACT ANALYSIS SUMMARY MATRIX

IMPACT	EFFECT: Unavailability of resource will result in …	UNAVAILABLE
Catastrophic	*describe the impact to the enterprise mission and/or delivery of client services if the resource is not available*	*insert time period that corresponds to each impact class*
Significant		
Minimal		
None		

MISSION SENSITIVITY

CODE	RESOURCE
Direct	directly supports the enterprise mission and delivery of client services
Indirect	indirectly supports the enterprise mission and delivery of client services
Subord	is subordinate to a direct or indirect resource and is an essential component to a direct/indirect resource
Fiscal	is related to monetary issues such as budget, revenue, expense, etc.
Admin	supports administrative functions such as employee benefits, payroll, timekeeping, record keeping, management, etc.

Sources used to generate tables: RMI Risk Management Institute
NIST National Institute of Standards and Technology, special publication 800-30
FCMS Federal Dept of Health & Human Services, Center for Medicare & Medicaid Services (CMS)

DETERMINING PROBABILITY VALUE

Value	RMI	NIST (likelihood)	FCMS (likelihood of occurrence)
High	Probable Has occurred recently or Has the potential of occurring several times in a given time period (2, 3, 5 years) or Likely to occur each year or More than a 25% chance of occurrence	Threat source is highly motivated & sufficiently capable and controls to prevent vulnerability from being exercised are ineffective	*Extreme*: Likely to occur multiple times per day *Very High*: Likely to occur multiple times per month *High*: Likely to occur once per month or less.
Moderate	Possible Has a history of occurrence or Could occur more than once within a given time period or Likely to occur in a 10 year period or Less than a 25% chance of occurrence or Could be difficult to control due to external influences	Threat source is motivated & capable but controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised	*Moderate*: Likely to occur once every 6 months or less
Low	Remote Has not occurred or Is unlikely to occur or Not likely to occur in a 10 year period or Less than a 2% chance of occurrence	Threat source lacks motivation or capability or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised	*Low*: Likely to occur once every year or less *Very Low*: Likely to occur 2 to 3 times every 5 years *Negligible*: Unlikely to occur

DETERMINING IMPACT VALUE

Value	RMI (consequence)	NIST	FCMS
High	Financial impact likely to exceed $_____. Significant impact on strategy, mission, or operational activities Significant stakeholder and/or citizen concerns (State terminology: ability to deliver services and meet the agency mission. Significant citizen and client concern).	High cost loss of major tangible assets or resources Significantly violates, harms, or impedes the mission Human death or serious injury may occur	*Critical* may cause extended or permanent outage; complete compromise of information or services; resumption at a hot site
			Serious may cause considerable outage or loss of business confidence; compromise of large amt of information or services
			Damaging may cause damage to reputation or loss of confidence in resource or service; requires significant expenditure to repair
Moderate	Financial impact likely to range between $_____ and $____. Moderate impact on strategy, mission, or operational activities Moderate stakeholder and/or citizen concerns	Costly loss of tangible assets or resources Violates, harms, or impedes the mission Human injury may result	*Significant* results in tangible harm, political embarrassment; requires some expenditure to repair
Low	Financial impact likely to be less than $_____. Minimal impact on strategy, mission, or operational activities Minimal stakeholder and/or citizen concerns	Loss of some tangible assets or resources Noticeably affects the mission	*Minor* minor effects requiring minimal effort to repair
			Insignificant almost no impact

DETERMINING RISK LEVEL VALUE

RMI: Risk analysis results used to produce a risk profile which ranks each risk & provides a tool for prioritizing risk treatment efforts.
FCMS: Mathematically, RISK LEVEL equals the Likelihood of Occurrence multiplied by Severity of Impact in the system's confidentiality, integrity, & availability. Risk may move to a higher level depending on security level & level of compromise if a threat is realized.

NIST: Risk Level Matrix

		IMPACT				
		High	Moderate	Low		
PROBABILITY	Value	100	50	10	**RISK LEVEL**	**NECESSARY ACTION**
High	1.0	High 100*1= 100	Mod 50*1= 50	Low 10*1= 10	gt 50 – 100 High	Correction action must be taken as soon as possible
Moderate	0.5	Mod 100*0.5= 50	Mod 50*0.5= 25	Low 10*0.5=5	gt 10 - 50 Moderate	Correction action plan developed & implemented within a reasonable amt of time
Low	0.1	Low 100*0.1= 10	Low 50*0.1= 5	Low 10*0.1=1	1 - 10 Low	Determine whether corrective action is warranted or decide to accept the risk

FCMS: Risk Level Matrix

		IMPACT					
		High			Moderate	Low	
PROBABILITY		Critical	Serious	Damaging	Significant	Minor	Insignificant
High	Extreme	High			High	Moderate	Low
	Very High						
	High						
Moderate	Moderate	High	High	High	Moderate	Low	Low
Low	Low	High	High	Moderate	Moderate	Low	
	Very Low	Moderate	Moderate	Low			
	Negligible	Low					

In addition, the American Health Information Management Association (AHIMA) lists the following as their determination of risk level., which they refer to as "Risk Ranking Scale". AHIMA also refers to impact as "criticality" with definitions listed in the table below.

AHIMA suggests that criticality be based on the amount of time a system could be down before:
patient care would be affected (high criticality)
operations would be significantly impacted (medium/moderate criticality), and
paper/independent computer systems would be used to load batches at a later time (low criticality)

AHIMA Probability & Impact (criticality) Definitions

Value	Probability	Impact	
High	Have experienced an incident Controls not effective	Results in human death or serious injury Inability to recover critical data High cost of recovery	Major lawsuit Loss of licensure or accreditation
Moderate	Have been alerted to threat controls may impede threat	Results in human injury or harm Complaint to federal government Significant cost of recovery	Minor lawsuit Public relations issue
Low	No one in the community has experienced threat Controls greatly deter or prevent threat success	Complaint Loss of productivity	Nuisance Embarrassment

AHIMA Risk Level (Score) Definition (Risk Ranking Scale)

	Impact (Criticality)		
Probability	High	Moderate	Low
High	9	6	3
Moderate	6	4	2
Low	3	2	1

RECOVERY TIME OBJECTIVE
HOURLY COMPARISON CHART

HOURS	DAYS	WEEKS	MONTHS	PERIODIC
24	1			
48	2			
72	3			
168	7	1		
336	14	2		
504	21	3		
672	28	4	1	Monthly
1344	56	8	2	
2016	84	12	3	Quarterly
8736	364	52	12	Annually

REVISION HISTORY

Created: May 1, 2006
Revised: Nov 20, 2006 / Oct 24, 2006 / June 26, 2006 / 12/18/2006
Reviewed: Nov 20, 2006
Effective: Jan 30, 2007

- End of Shared Services Glossary -